

PCT

RAPPORT DE RECHERCHE INTERNATIONALE

(article 18 et règles 43 et 44 du PCT)

Référence du dossier du déposant ou du mandataire GEM 498	POUR SUITE voir la notification de transmission du rapport de recherche internationale (formulaire PCT/ISA/220) et, le cas échéant, le point 5 ci-après A DONNER	
Demande internationale n° PCT/FR 99/ 00583	Date du dépôt international (jour/mois/année) 16/03/1999	(Date de priorité (la plus ancienne) (jour/mois/année) 20/03/1998
Déposant GEMPLUS S.C.A. et al.		

Le présent rapport de recherche internationale, établi par l'administration chargée de la recherche internationale, est transmis au déposant conformément à l'article 18. Une copie en est transmise au Bureau international.

Ce rapport de recherche internationale comprend 3 feuilles.

☒ Il est aussi accompagné d'une copie de chaque document relatif à l'état de la technique qui y est cité.

1. Base du rapport

- a. En ce qui concerne la **langue**, la recherche internationale a été effectuée sur la base de la demande internationale dans la langue dans laquelle elle a été déposée, sauf indication contraire donnée sous le même point.
- ☐ la recherche internationale a été effectuée sur la base d'une traduction de la demande internationale remise à l'administration.
- b. En ce qui concerne les **séquences de nucléotides ou d'acides aminés** divulguées dans la demande internationale (le cas échéant), la recherche internationale a été effectuée sur la base du listage des séquences :
- ☐ contenu dans la demande internationale, sous forme écrite.
- ☐ déposée avec la demande internationale, sous forme déchiffrable par ordinateur.
- ☐ remis ultérieurement à l'administration, sous forme écrite.
- ☐ remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur.
- ☐ La déclaration, selon laquelle le listage des séquences présenté par écrit et fourni ultérieurement ne vas pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie.
- ☐ La déclaration, selon laquelle les informations enregistrées sous forme déchiffrable par ordinateur sont identiques à celles du listage des séquences présenté par écrit, a été fournie.

2. ☐ **Il a été estimé que certaines revendications ne pouvaient pas faire l'objet d'une recherche** (voir le cadre I).

3. ☐ **Il y a absence d'unité de l'invention** (voir le cadre II).

4. En ce qui concerne le **titre**,

- ☒ le texte est approuvé tel qu'il a été remis par le déposant.
- ☐ Le texte a été établi par l'administration et a la teneur suivante:

5. En ce qui concerne l'**abrégé**,

- ☒ le texte est approuvé tel qu'il a été remis par le déposant
- ☐ le texte (reproduit dans le cadre III) a été établi par l'administration conformément à la règle 38.2b). Le déposant peut présenter des observations à l'administration dans un délai d'un mois à compter de la date d'expédition du présent rapport de recherche internationale.

6. La figure **des dessins** à publier avec l'abrégé est la Figure n°

- ☒ suggérée par le déposant.
- ☐ parce que le déposant n'a pas suggéré de figure.
- ☐ parce que cette figure caractérise mieux l'invention.

1
☐ Aucune des figures n'est à publier.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/FR 99/00583

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 4295041	A	13-10-1981	FR 2401459 A	23-03-1979
			FR 2460506 A	23-01-1981
			CH 631561 A	13-08-1982
			DE 2837201 A	01-03-1979
			DE 2858818 C	29-08-1996
			DE 2858819 C	09-03-1995
			DE 2858829 C	28-11-1996
			GB 2004394 A,B	28-03-1979
			JP 54046447 A	12-04-1979
			JP 62056556 B	26-11-1987
			JP 2506061 B	12-06-1996
			JP 7093501 A	07-04-1995
			JP 1826230 C	28-02-1994
			JP 2210590 A	21-08-1990
			JP 3050314 B	01-08-1991
			JP 1556417 C	23-04-1990
			JP 62070993 A	01-04-1987
			JP 63025393 B	25-05-1988
			JP 2097860 C	02-10-1996
			JP 5217034 A	27-08-1993
			JP 8007780 B	29-01-1996
			US 4211919 A	08-07-1980
			DE 3025044 A	27-05-1981
			JP 56038651 A	13-04-1981
			JP 2547379 B	23-10-1996
			JP 8110937 A	30-04-1996
			JP 1152589 A	15-06-1989
			JP 2043222 B	27-09-1990
			JP 2547368 B	23-10-1996
			JP 5274499 A	22-10-1993
US 4932053	A	05-06-1990	FR 2638869 A	11-05-1990
			EP 0368727 A	16-05-1990
			JP 2199561 A	07-08-1990
			JP 2813663 B	22-10-1998
US 4813024	A	14-03-1989	FR 2600183 A	18-12-1987
			DE 3777701 A	30-04-1992
			EP 0251853 A	07-01-1988
			JP 63080351 A	11-04-1988
WO 9606504	A	29-02-1996	AU 3238595 A	22-03-1996
			AU 701593 B	04-02-1999
			AU 3239495 A	14-03-1996
			BR 9508621 A	30-09-1997
			BR 9508622 A	19-05-1998
			CA 2196406 A	07-03-1996
			CA 2196407 A	29-02-1996
			CN 1158202 A	27-08-1997
			CN 1158203 A	27-08-1997
			EP 0878088 A	18-11-1998
			EP 0782807 A	09-07-1997
			FI 970677 A	18-02-1997
			JP 10506507 T	23-06-1998
			JP 10505720 T	02-06-1998
			PL 318647 A	07-07-1997
			WO 9607267 A	07-03-1996

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale No

PCT/FR 99/00583

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
CIB 6 G06K19/073

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)

CIB 6 G07F G06K G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si réalisable, termes de recherche utilisés)

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie °	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 4 295 041 A (UGON MICHEL) 13 octobre 1981 voir abrégé; revendication 1; figures 1,2 voir colonne 1, ligne 61 - colonne 2, ligne 21	1,5,7
X	US 4 932 053 A (FRUHAUF SERGE ET AL) 5 juin 1990	1,3,4,7
Y	voir abrégé; figure 4 voir colonne 2, ligne 29-59 voir colonne 3, ligne 26 - colonne 4, ligne 21	6

☒ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

° Catégories spéciales de documents cités:

- "A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent
- "E" document antérieur, mais publié à la date de dépôt international ou après cette date
- "L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)
- "O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens
- "P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée

15 juin 1999

Date d'expédition du présent rapport de recherche internationale

21/06/1999

Nom et adresse postale de l'administration chargée de la recherche internationale

Office Européen des Brevets, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Fonctionnaire autorisé

Cardigos dos Reis, F

C.(suite) DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 4 813 024 A (LISIMAQUE GILLES ET AL) 14 mars 1989	1,5,7
Y	voir colonne 2, ligne 8-31 voir colonne 3, ligne 63 - colonne 4, ligne 13 voir colonne 6, ligne 18-22	6,8,9
Y	WO 96 06504 A (CHANEY JOHN WILLIAM ; THOMSON CONSUMER ELECTRONICS (US)) 29 février 1996 voir page 1, ligne 5-20 voir page 2, ligne 3-10 voir page 13, ligne 8-20 voir page 22, ligne 9-18	8,9

TRAITE DE COOPERATION EN MATIERE BREVETS

PCT

NOTIFICATION D'ELECTION

(règle 61.2 du PCT)

Expéditeur: le BUREAU INTERNATIONAL

Destinataire:

Assistant Commissioner for Patents
United States Patent and Trademark
Office
Box PCT
Washington, D.C.20231
ÉTATS-UNIS D'AMÉRIQUE

en sa qualité d'office élu

Date d'expédition (jour/mois/année)
11 octobre 1999 (11.10.99)

Demande internationale no
PCT/FR99/00583

Référence du dossier du déposant ou du mandataire
GEM 498

Date du dépôt international (jour/mois/année)
16 mars 1999 (16.03.99)

Date de priorité (jour/mois/année)
20 mars 1998 (20.03.98)

Déposant

FEYT, Nathalie etc

1. L'office désigné est avisé de son élection qui a été faite:



dans la demande d'examen préliminaire international présentée à l'administration chargée de l'examen préliminaire international le:

10 septembre 1999 (10.09.99)



dans une déclaration visant une élection ultérieure déposée auprès du Bureau international le:

2. L'élection



a été faite



n'a pas été faite

avant l'expiration d'un délai de 19 mois à compter de la date de priorité ou, lorsque la règle 32 s'applique, dans le délai visé à la règle 32.2b).

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur: (41-22) 740.14.35

Fonctionnaire autorisé

Kiwa Mpay

no de téléphone: (41-22) 338.83.38

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

NOTIFICATION DE L'ENREGISTREMENT D'UN CHANGEMENT

(règle 92bis.1 et
instruction administrative 422 du PCT)

Expéditeur: le BUREAU INTERNATIONAL

Destinataire:

NONNENMACHER, Bernard
Gemplus
avenue du Pic de Bertagne
Parc d'Activités de Gémenos
F-13881 Gémenos Cedex
FRANCE

Date d'expédition (jour/mois/année) 12 juillet 2000 (12.07.00)	NOTIFICATION IMPORTANTE
Référence du dossier du déposant ou du mandataire GEM 498	
Demande internationale no PCT/FR99/00583	Date du dépôt international (jour/mois/année) 16 mars 1999 (16.03.99)

1. Les renseignements suivants étaient enregistrés en ce qui concerne:

☒ le déposant ☐ l'inventeur ☐ le mandataire ☐ le représentant commun

Nom et adresse

GEMPLUS S.C.A.
avenue du Pic de Bertagne
Parc d'Activités de Gémenos
Boîte postale 100
F-13881 Gémenos Cedex
FRANCE

Nationalité (nom de l'Etat)

FR

Domicile (nom de l'Etat)

FR

no de téléphone

no de télécopieur

no de téléimprimeur

2. Le Bureau international notifie au déposant que le changement indiqué ci-après a été enregistré en ce qui concerne:

☐ la personne ☒ le nom ☐ l'adresse ☐ la nationalité ☐ le domicile

Nom et adresse

GEMPLUS
avenue du Pic de Bertagne
Parc d'Activités de Gémenos
Boîte postale 100
F-13881 Gémenos Cedex
FRANCE

Nationalité (nom de l'Etat)

FR

Domicile (nom de l'Etat)

FR

no de téléphone

no de télécopieur

no de téléimprimeur

3. Observations complémentaires, le cas échéant:

4. Une copie de cette notification a été envoyée:

☒ à l'office récepteur ☐ aux offices désignés concernés
☐ à l'administration chargée de la recherche internationale ☒ aux offices élus concernés
☒ à l'administration chargée de l'examen préliminaire international ☐ autre destinataire:

Bureau international de l'OMPI
34, chemin des Colombettes
1211 Genève 20, Suisse

no de télécopieur (41-22) 740.14.35

Fonctionnaire autorisé:

Simin Baharlou

no de téléphone (41-22) 338.83.38

TRAITE DE COOPERATION EN MATIERE DE BREVETS

PCT

REC'D 19 MAY 2000
WIPO

RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL^{PCT}

(article 36 et règle 70 du PCT)



Référence du dossier du déposant ou du mandataire GEM 498	POUR SUITE A DONNER voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)	
Demande internationale n° PCT/FR99/00583	Date du dépôt international (jour/mois/année) 16/03/1999	Date de priorité (jour/mois/année) 20/03/1998
Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB G06K19/073		
Déposant GEMPLUS S.C.A. et al.		

- Le présent rapport d'examen préliminaire international, établi par l'administration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.
- Ce RAPPORT comprend 7 feuilles, y compris la présente feuille de couverture.
 - ☐ Il est accompagné d'ANNEXES, c'est-à-dire de feuilles de la description, des revendications ou des dessins qui ont été modifiées et qui servent de base au présent rapport ou de feuilles contenant des rectifications faites auprès de l'administration chargée de l'examen préliminaire international (voir la règle 70.16 et l'instruction 607 des Instructions administratives du PCT).

Ces annexes comprennent feuilles.

- Le présent rapport contient des indications relatives aux points suivants:

- I ☒ Base du rapport
- II ☐ Priorité
- III ☒ Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle
- IV ☒ Absence d'unité de l'invention
- V ☒ Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
- VI ☐ Certains documents cités
- VII ☒ Irrégularités dans la demande internationale
- VIII ☐ Observations relatives à la demande internationale

Date de présentation de la demande d'examen préliminaire internationale 10/09/1999	Date d'achèvement du présent rapport 17.05.2000
Nom et adresse postale de l'administration chargée de l'examen préliminaire international:  Office européen des brevets D-80298 Munich Tél. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Fonctionnaire autorisé Koegler, L N° de téléphone +49 89 2399 2785 

**RAPPORT D'EXAMEN
PRELIMINAIRE INTERNATIONAL**

Demande internationale n° PCT/FR99/00583

I. Base du rapport

1. Ce rapport a été rédigé sur la base des éléments ci-après (*les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées, dans le présent rapport, comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications.*) :

Description, pages:

1-6 version initiale

Revendications, N°:

1-9 version initiale

Dessins, feuilles:

1-3 version initiale

2. Les modifications ont entraîné l'annulation :

☐ de la description, pages :

☐ des revendications, n°s :

☐ des dessins, feuilles :

3. ☐ Le présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été considérées comme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après (règle 70.2(c)) :

4. Observations complémentaires, le cas échéant :

III. Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle

La question de savoir si l'objet de l'invention revendiquée semble être nouveau, impliquer une activité inventive (ne pas être évident) ou être susceptible d'application industrielle n'a pas été examinée pour ce qui concerne :

☐ l'ensemble de la demande internationale.

☒ les revendications n°s 9.

**RAPPORT D'EXAMEN
PRELIMINAIRE INTERNATIONAL**

Demande internationale n° PCT/FR99/00583

parce que :

- ☐ la demande internationale, ou les revendications n°s en question, se rapportent à l'objet suivant, à l'égard duquel l'administration chargée de l'examen préliminaire international n'est pas tenue d'effectuer un examen préliminaire international (*préciser*) :
- ☒ la description, les revendications ou les dessins (*en indiquer les éléments ci-dessous*), ou les revendications n°s 9 en question ne sont pas claires, de sorte qu'il n'est pas possible de formuler une opinion valable (*préciser*) :
voir feuille séparée
- ☐ les revendications, ou les revendications n°s en question, ne se fondent pas de façon adéquate sur la description, de sorte qu'il n'est pas possible de formuler une opinion valable.
- ☐ il n'a pas été établi de rapport de recherche internationale pour les revendications n°s en question.

IV. Absence d'unité de l'invention

1. En réponse à l'invitation à limiter les revendications ou à payer des taxes additionnelles, le déposant a
 - ☐ limité les revendications.
 - ☐ payé des taxes additionnelles.
 - ☐ payé des taxes additionnelles sous réserve.
 - ☒ ni limité les revendications ni payé des taxes additionnelles.
2. ☐ L'administration chargée de l'examen préliminaire international estime qu'il n'est pas satisfait à l'exigence d'unité d'invention et décide, conformément à la règle 68.1, de ne pas inviter le déposant à limiter les revendications ou à payer des taxes additionnelles.
3. L'administration chargée de l'examen préliminaire international estime que, aux termes des règles 13.1, 13.2 et 13.3,
 - ☐ il est satisfait à l'exigence d'unité de l'invention.
 - ☒ il n'est pas satisfait à l'exigence d'unité de l'invention, et ce pour les raisons suivantes :
voir feuille séparée
4. En conséquence, les parties suivantes de la demande internationale ont fait l'objet d'un examen préliminaire international lors de la formulation du présent rapport :
 - ☒ toutes les parties de la demande.

**RAPPORT D'EXAMEN
PRELIMINAIRE INTERNATIONAL**

Demande internationale n° PCT/FR99/00583

☐ les parties relatives aux revendications n^{os}.

V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Déclaration

Nouveauté	Oui : Revendications 2,8
	Non : Revendications 1,3-5
Activité inventive	Oui : Revendications 2,8
	Non : Revendications 6,7
Possibilité d'application industrielle	Oui : Revendications 1-8
	Non : Revendications

2. Citations et explications

voir feuille séparée

VII. Irrégularités dans la demande internationale

Les irrégularités suivantes, concernant la forme ou le contenu de la demande internationale, ont été constatées :

voir feuille séparée

Concernant le point III

Absence de formulation d'opinion quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle

La revendication 9 indépendante n'est pas claire (Art. 6 PCT) parce qu'elle cite des éléments (pompe de charge etc.) qui ne sont pas définis dans la revendication de procédé elle-même, mais seulement dans la revendication 8.

Concernant le point IV

Absence d'unité de l'invention

L'objet de la revendication indépendante 1 est déjà connu (cf. les motifs de cette objection). L'exigence d'unité de l'invention (règle 13.1 PCT) n'est donc pas observée, dans la mesure où il n'existe pas entre les objets des groupes suivants de revendications dépendantes de relation technique portant sur un ou plusieurs éléments techniques particuliers identiques ou correspondants au sens de la règle 13.2 PCT:

Revendication 2: Utilisation d'un intégrateur pour moyenner les variations du courant consommé

Revendications 8 et 9: Ecriture des données aléatoires pendant le calcul cryptographique

Concernant le point V

Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

1. Il est fait référence aux documents suivants:

D1: US-A-4 932 053 (FRUHAUF SERGE ET AL) 5 juin 1990

D2: US-A-4 295 041 (UGON MICHEL) 13 octobre 1981

D3: US-A-4 813 024 (LISIMAQUE GILLES ET AL) 14 mars 1989

D4: WO 96 06504 A (CHANEY JOHN WILLIAM ; THOMSON CONSUMER ELECTRONICS (US)) 29 février 1996

2. Le document D1 divulgue toutes les caractéristiques des revendications 1 et 3 à 5:

Un dispositif pour masquer les opérations effectuées par un composant destiné à être intégré à une carte à puce (D1 col. 1 lignes 7-65), caractérisé en ce qu'il comprend au moins un moyen (Fig. 1, BD1/T1 - BD3/T3) pour modifier la consommation de courant dudit composant lors de la réalisation desdites opérations (D1, col. 2 lignes 29 - 45).

Le dispositif comprend au moins un générateur de signaux aléatoires (GPA dans la Fig. 1) et une batterie de résistances (T'1 - T'3) dont l'alimentation de chacune des résistances est commandée par les signaux aléatoires (S1-S3).

Le dispositif comprend une pluralité de moyens (BD1/T1, BD2/T2, BD3/T3) pour modifier la consommation de courant.

Le moyen pour modifier la consommation de courant dans le cas d'une mémoire EEPROM (D1, col. 4, lignes 5-21) consiste à effectuer simultanément une opération d'écriture ou d'effacement de la mémoire dite de masquage et une opération du microprocesseur (D1: col. lignes 23-30; col. 4 lignes 5-21; évidemment une opération de microprocesseur est nécessaire pour écrire la mémoire EEPROM)

Par conséquent, le sujet des revendications 1 et 3 à 5 n'est pas nouveau.

3. Les revendications 6 et 7 ne sont pas inventives pour les raisons suivantes:

Les cellules T1 à T3 selon le document D1 n'enregistrent pas vraiment les données aléatoires parce que les grilles flottantes sont connectées aux grilles de contrôle. Néanmoins, D2 divulgue l'utilisation d'une vraie cellule de mémoire à cet effet, ce qui est une alternative évidente à l'utilisation des transistors modifiés.

Afin de minimiser la consommation d'énergie, il est évident d'utiliser les moyens pour modifier le courant seulement pendant les opérations à sécuriser.

4. L'art antérieur ne suggère pas d'effectuer le calcul cryptographique pendant l'écriture des données aléatoires afin de sécuriser le calcul en modifiant la consommation de courant (revendication 8). Les documents D1 à D3 ne concernent que la protection des opérations d'écriture par modification du courant consommé. Le document D4 ne concerne pas l'aspect de surveillance du courant consommé par la carte. Le circuit intégrateur selon la revendication 2 n'est pas non plus suggéré par ces documents.

Concernant le point VII

Irrégularités dans la demande internationale

La revendication indépendante 1 n'est pas formulée comme prévu par la règle 6.3 b) PCT, alors qu'une telle présentation semblerait appropriée en l'espèce, les caractéristiques connues en combinaison de l'état de la technique selon document D1 figurant dans le préambule (règle 6.3 b) i) PCT) et les caractéristiques restantes figurant dans la partie caractérisante (règle 6.3 b) ii) PCT).

Contrairement à ce qu'exige la règle 5.1 a) ii) PCT, la description n'indique pas l'état de la technique antérieure pertinent exposé dans les documents D1 à D4 et ne cite pas ces documents.

Translation
09646564
5060

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

4

Applicant's or agent's file reference GEM 498	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/FR99/00583	International filing date (day/month/year) 16 March 1999 (16.03.99)	Priority date (day/month/year) 20 March 1998 (20.03.98)
International Patent Classification (IPC) or national classification and IPC G06K 19/073		
Applicant GEMPLUS		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 7 sheets, including this cover sheet.

☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

These annexes consist of a total of _____ sheets.

3. This report contains indications relating to the following items:

- I ☒ Basis of the report
- II ☐ Priority
- III ☒ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- IV ☒ Lack of unity of invention
- V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- VI ☐ Certain documents cited
- VII ☒ Certain defects in the international application
- VIII ☐ Certain observations on the international application

Date of submission of the demand 10 September 1999 (10.09.99)	Date of completion of this report 17 May 2000 (17.05.2000)
Name and mailing address of the IPEA/EP	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR99/00583

I. Basis of the report

1. This report has been drawn on the basis of *(Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.)*:

- ☐ the international application as originally filed.
- ☒ the description, pages 1-6, as originally filed,
 pages _____, filed with the demand,
 pages _____, filed with the letter of _____,
 pages _____, filed with the letter of _____.
- ☒ the claims, Nos. 1-9, as originally filed,
 Nos. _____, as amended under Article 19,
 Nos. _____, filed with the demand,
 Nos. _____, filed with the letter of _____,
 Nos. _____, filed with the letter of _____.
- ☒ the drawings, sheets/fig 1-3, as originally filed,
 sheets/fig _____, filed with the demand,
 sheets/fig _____, filed with the letter of _____,
 sheets/fig _____, filed with the letter of _____.

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages _____
- ☐ the claims, Nos. _____
- ☐ the drawings, sheets/fig _____

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

4. Additional observations, if necessary:

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

international application No.

PCT/FR99/00583

III. Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non obvious), or to be industrially applicable have not been examined in respect of:

☐ the entire international application.

☒ claims Nos. 9

because:

☐ the said international application, or the said claims Nos. _____
relate to the following subject matter which does not require an international preliminary examination (*specify*):

☒ the description, claims or drawings (*indicate particular elements below*) or said claims Nos. 9
are so unclear that no meaningful opinion could be formed (*specify*):

See the Supplemental Box.

☐ the claims, or said claims Nos. _____ are so inadequately supported
by the description that no meaningful opinion could be formed.

☐ no international search report has been established for said claims Nos. _____

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/FR 99/00583

Supplemental Box

(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: III

Independent claim 9 is not clear (PCT Article 6) because it cites components (charge pump, etc.) that are not defined in the method claim itself, but only in claim 8.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/FR99/00583

IV. Lack of unity of invention

1. In response to the invitation to restrict or pay additional fees the applicant has:

- ☐ restricted the claims.
- ☐ paid additional fees.
- ☐ paid additional fees under protest.
- ☒ neither restricted nor paid additional fees.

2. ☐ This Authority found that the requirement of unity of invention is not complied with and chose, according to Rule 68.1, not to invite the applicant to restrict or pay additional fees.

3. This Authority considers that the requirement of unity of invention in accordance with Rules 13.1, 13.2 and 13.3 is

- ☐ complied with.
- ☒ not complied with for the following reasons:

See the Supplemental Box.

4. Consequently, the following parts of the international application were the subject of international preliminary examination in establishing this report:

- ☒ all parts.
- ☐ the parts relating to claims Nos. _____

Supplemental Box

(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: IV

The subject matter of independent claim 1 is already known (cf. the reasons for this objection). The unity of invention requirement (PCT Rule 13.1) has therefore not been met, since no technical relationship exists between the subjects of the following groups of dependent claims involving one or more of the same or corresponding special technical features, within the meaning of PCT Rule 13.2:

Claim 2: Using an integrator for averaging variations in the current consumed,

Claims 8 and 9: Writing random data during cryptographic calculation.

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	2, 8	YES
	Claims	1, 3-5	NO
Inventive step (IS)	Claims	2, 8	YES
	Claims	6, 7	NO
Industrial applicability (IA)	Claims	1-8	YES
	Claims		NO

2. Citations and explanations

1. Reference is made to the following documents:

D1: US-A-4 932 053 (FRUHAUF SERGE ET AL) 5 June 1990

D2: US-A-4 295 041 (UGON MICHEL) 13 October 1981

D3: US-A-4 813 024 (LISIMAQUE GILLES ET AL) 14 March 1989

D4: WO 96 06504 A (CHANEY JOHN WILLIAM; THOMSON CONSUMER ELECTRONICS (US)) 29 February 1996

2. Document D1 discloses all the features of claims 1 and 3 through 5:

A device for masking operations performed by a component to be integrated into a chip card (D1 column 1, lines 7-65), characterized in that it includes at least one means (figure 1, BD1/T1 - BD3/T3) for modifying the current consumption of said component while said operations are carried out (D1, column 2, lines 29-45).

The device includes at least one random signal generator (GPA in figure 1) and a bank of resistors (T'1 - T'3) in which the power supply of each resistor is controlled by the random signals (S1 -

S3).

The device includes a plurality of means (BD1/T1, BD2/T2, BD3/T3) for modifying the current consumption.

The means for modifying current consumption in the case of an EEPROM memory (D1, column 4, lines 5-21) comprises simultaneously performing a memory writing or erasing operation, known as masking, and a microprocessor operation (D1, lines 23-30, column 4, lines 5-21; a microprocessor operation is obviously necessary for writing the EEPROM memory).

Therefore, the subject matter of claims 1 and 3 through 5 is not novel.

3. Claims 6 and 7 are not inventive for the following reasons:

The T1 to T3 cells according to document D1 do not really record the random data because the floating gates are connected to the control gates. Nevertheless, D2 discloses using a real storage cell for this purpose, which is an obvious alternative to the use of modified transistors. In order to minimize energy consumption, it is obvious to use means for modifying the current only during operations to be made secure.

4. The prior art does not suggest performing the cryptographic calculation during the writing of random data in order to secure the calculation by modifying the current consumption (claim 8).

Documents D1 through D3 merely relate to protecting

writing operations by modifying the current consumption. Document D4 does not relate to the aspect of monitoring the current consumed by the card. The integrator circuit according to claim 2 is not suggested by these documents either.

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

Independent claim 1 has not been drafted in the two-part form, as provided for by PCT Rule 6.3(b), even though it would appear appropriate to do so in this case. The features known in combination from the prior art according to document D1 should be included in the preamble (PCT Rule 6.3(b)(i)) and the remaining features in the characterizing part (PCT Rule 6.3(b)(ii)).

Contrary to the requirements of PCT Rule 5.1(a)(ii), the relevant prior art disclosed in documents D1 through D4 has not been indicated in the description, nor have these documents been cited.